Council of the
European Union

Brussels, 31 July 2020
(OR. en)

10048/20

HYBRID 24
DISINFO 20
AG 38
PE 46
DATAPROTECT 74
JAI 629
CYBER 143
JAIEX 74
FREMP 53
RELEX 574
CULT 37
EDUC 289
AUDIO 26
DIGIT 65
INF 148
COSI 124
CSDP/PSDC 394
COPS 261
POLMIL 104
IPCR 21
PROCIV 51
CSC 221

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2020) 152 final
Subject:	JOINT STAFF WORKING DOCUMENT Mapping of measures related to enhancing resilience and countering hybrid threats

Delegations will find attached document SWD(2020) 152 final.

Encl.: SWD(2020) 152 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 24.7.2020
SWD(2020) 152 final

JOINT STAFF WORKING DOCUMENT

Mapping of measures related to enhancing resilience and countering hybrid threats

Mapping of measures related to enhancing resilience and countering hybrid threats

The first steps of the EU work on hybrid threats date back to 2015, when Council adopted conclusions on Common Defence and Security Policy (CSDP) calling for a joint framework with actionable proposals to help counter hybrid threats and foster the resilience of the EU and Member States, as well as partners. The first comprehensive policy document, *Joint Framework on countering hybrid threats – a European Union response*[1] was issued in 2016. As threats and challenges had rapidly evolved, in 2018, the Commission and the High Representative presented *Joint Communication on increasing resilience and bolstering capabilities to counter hybrid threats*[2]. In addition, the EU policy on countering hybrid threats has been subject to numerous Council Conclusions.

On 10 December 2019, *Council Conclusions on complementary efforts to enhance resilience and counter hybrid threats*[3] were adopted. Paragraph 17 of these Council Conclusions invited the Commission and the High Representative '*to produce a mapping that would take into account the measures taken so far and the relevant documents adopted in a comprehensive fashion, with a view to possible new initiatives'*.

The objective of the present mapping is to provide a comprehensive inventory of countering hybrid threats-related measures at EU level and to list the corresponding policy and legal documents. Since the adoption in 2016 of the Joint Framework, almost 200 measures related to increasing resilience and countering hybrid threats have been implemented by the Commission and High Representative in cooperation with the Member States and the relevant stakeholders, as appropriate. Beyond these, the mapping also includes measures relevant to countering hybrid threats, whose establishment precedes the 2016 Joint Framework, like for example the creation in 2015 of the East StratCom Task Force, as well as measures stemming from *The European Agenda on Security* adopted in 2015[4].

Based on the present mapping, a restricted online platform will be created for Member States' easy reference on counter-hybrid tools and measures at EU level. The platform will be updated as new measures are established.

The mapping is a joint work of the Commission services and the European External Action Service, incorporating the valuable contribution from the European Defence Agency. The document will be presented to Member States in the Horizontal Working Party Enhancing Resilience and Countering Hybrid Threats.

[1] JOIN(2016) 18 final.

[2] JOIN(2018) 16 final.

[3] Council document ST 14972/19.

[4] COM(2015) 185.

Table of contents:

1. Primary documents on countering hybrid threats	
EU institutions	**Member States**
Joint Framework on countering hybrid threats – a European Union response, JOIN(2016) 18 final Joint Communication on increasing resilience and bolstering capabilities to counter hybrid threats, JOIN(2018) 16 final Annual progress reports on countering hybrid threats: JOIN(2017) 30 final, JOIN(2018) 14 final, SWD(2019) 200 final, SWD(2020) 153 final The European Agenda on Security, COM(2015) 185 and progress reports[5] EU operational protocol for countering hybrid threats "EU Playbook", SWD(2016) 227 final	Council Conclusions on Common Defence and Security Policy (CSDP), May 2015 [Consilium 8971/15][6] European Council Conclusions, June 2015 [EUCO 22/15][7] EUCO 2015 EUCO 11/15[8] Conclusions on Countering Hybrid Threats of 19 April 2016[9] EUCO March 2018 EUCO 1/18[10] CC June 2018 10496/18[11] EUCO June 2018 EUCO 9/18[12] EUCO December 2018 EUCO 17/18[13] EUCO March 2019 EUCO 1/19[14] EUCO June 2019 EUCO 9/19[15] Council Conclusions on complementary efforts to enhance resilience and counter hybrid threats, December 2019, Council document 14972/19[16] Council Conclusions on Security and Defence June 2020 8910/20[17]

[5] https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en.

[6] http://data.consilium.europa.eu/doc/document/ST-8971-2015-INIT/en/pdf.

[7] https://www.consilium.europa.eu/media/21717/euco-conclusions-25-26-june-2015.pdf.

[8] https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.

[9] https://www.consilium.europa.eu/en/press/press-releases/2016/04/19/fac-conclusions-hybrid-threats/.

[10] https://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf.

[11] http://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.

[12] https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.

[13] https://www.consilium.europa.eu/media/37535/14-euco-final-conclusions-en.pdf.

[14] https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf.

[15] https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf.

[16] https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

[17] https://www.consilium.europa.eu/media/44521/st08910-en20.pdf.

2. National and pan-European vulnerabilities

Measure	Reference documents
Launching hybrid risk surveys in Member States	Operationalising Action 1 of the Joint Communication Countering Hybrid Threats by launching a hybrid risk survey in the Member States, Council document WK 7540/2017 REV 6 Implementation of Action 1 of the Joint Framework on countering hybrid threats - Presidency Report, Council document 10189/18
Analysis of national and pan-European vulnerabilities in structures and networks, following the first iteration of the survey	Preliminary analysis of Action 1 questionnaires and food for thought paper, JRC121144 Next Steps on the Preliminary analysis, Council document WK 839/2020 INIT

3. Situational awareness

Measure	Reference documents
Establishment of the EU Hybrid Fusion Cell	See Primary Documents on page 3
Establishment of the network of National Point of Contacts	See Primary Documents on page 3
Establishment of the network of Commission Points of Contact	See Primary Documents on page 3
Periodical Hybrid Trend Analysis presented to MS	See Primary Documents on page 3
Enhancement of the EU Hybrid Fusion Cell with appropriate resources and professional expertise	See Primary Documents on page 3
Periodical updates to MS in the Horizontal Working Party Enhancing Resilience and Countering Hybrid Threats on hybrid (HFC), cyber and disinformation (STRATCOM)	See Primary Documents on page 3
Strengthening internal coordination within EEAS including geographical departments to identify and alert on hybrid threats.	See Primary Documents on page 3

4. Strategic communications and countering disinformation

Measure	Reference documents
Establishment of East StratCom Task Force (2015) and subsequent establishment of Task Forces South and Western Balkans	Action Plan on Strategic Communications Ares(2015)2608242
Establishment of more proactive strategic communications and media monitoring	Action Plan on Strategic Communications Ares(2015)2608242 EP Preparatory Action
Launch and maintenance of the EUvsDisinfo.eu website	Action Plan on Strategic Communications Ares(2015)2608242
Action Plan against Disinformation	2019 Joint Communication on the Implementation of the Action Plan against Disinformation JOIN (2018) 36 final Presidency report on the mapping exercise concerning the actions undertaken at EU Member States level to combat disinformation (28 June 2019 WK 4894/2019 REV 3) 2020 Joint Communication on tackling COVID-19 disinformation – Getting facts right 10.6.2020 JOIN(2020) 8 final
Launching of a Rapid Alert System	Action Plan against Disinformation Terms of Reference of the Rapid Alert System
Reorganisation of the StratCom Division	Action Plan against Disinformation, 2018
Establishment of close coordination network and joint work on raising awareness on the disinformation among EU Institutions	Action Plan against Disinformation, 2018
Scoping and analysis of the phenomenon of disinformation and recommendations on measures and actions by the Commission and Member States	Final Report of the High Level Group on Fake News and Online Disinformation, A multi-dimensional approach to disinformation, 12 March 2018[18] Tackling Online Disinformation: a European Approach, COM(2018) 236 final Regular intelligence-based reporting by the EU Hybrid Fusion Cell
Creating a self-regulatory Code of Practice for online platforms and the advertising sector, with	Code of Practice on Disinformation for online platforms and the advertising

[18] https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

commitments undertaken by signatories to counter disinformation in the EU	sector, September 2018 Action Plan against Disinformation, JOIN (2018) 36 final Joint Communication on the Implementation of the Action Plan against Disinformation, JOIN(2019) 12 final
Stepping up implementation and monitoring of the Code of Practice in advance of the 2019 European elections , with the assistance of the European Regulators Group for Audio-visual Media Services (ERGA)	Action Plan against Disinformation, JOIN (2018) 36 final Joint Communication on the Implementation of the Action Plan against Disinformation, JOIN (2019) 12 final European Regulators Group for Audiovisual Media Services (ERGA), Intermediate Monitoring Report, June 2019[19] Monthly intermediate monitoring reports of the platform signatories[20]
Performing, with the assistance of the European Regulators Group for Audiovisual Media Services (ERGA), a comprehensive assessment of the effectiveness of the Code of Practice on Disinformation during its initial 12-months period of operations	European Regulators Group for Audiovisual Media Services (ERGA), Assessment of the implementation of the Code of Practice, May 2020[21] Study by Valdani Vicari & Associati (VVA), Assessment of the implementation of the Code of Practice on Disinformation, Final Report, May 2020[22] Annual self-assessment reports by signatories[23]
Supporting the creation of an independent network of European fact-checking organisations through the Observatory for Disinformation and Social Media Analysis (SOMA), an H2020 project	Tackling online disinformation: a European Approach, COM(2018) 236 final Report on the implementation of the Communication on Tackling online disinformation: a European Approach, COM(2018) 794 final

[19] https://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf.

[20] https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation, https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation, https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation, https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation, https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.

[21] https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.

[22] https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation.

[23] https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

	Website of the Observatory for Disinformation and Social Media Analysis (SOMA) [24]
Support to national multidisciplinary teams of fact-checkers and researchers to detect and expose disinformation campaign across social networks including putting in place a European Digital Media Observatory (EDMO), a secure infrastructure platform to enable better identification and detection of threats and potential manipulations	Tackling online disinformation: a European Approach, COM(2018) 236 final Joint Communication on the Implementation of the Action Plan against Disinformation, JOIN(2019) 12 final Website of the European Digital Media Observatory (EDMO)[25]
Use of Horizon 2020 funding to support technologies and tools to detect and analyse disinformation	Tackling online disinformation: a European Approach, COM (2018) 236 final Horizon 2020 Work Programme 2018-2020, Chapter 5.i. Information and Communication Technologies
Raising awareness and empowering citizens, including through fostering media literacy around disinformation, for instance by means of the European Media Literacy Week (18-22 March 2019)	Tackling online disinformation: a European Approach, COM (2018) 236 final
Support for quality journalism and media freedom and pluralism	Tackling online disinformation: a European Approach, COM(2018) 236 final Pilot projects co-funded by the European Commission, with the support of the European Parliament[26]
Mapping of Member States actions to combat disinformation	Presidency report on the mapping exercise concerning the actions undertaken at EU Member States level to combat disinformation, Council document WK 4894/2019 REV 3
Stepping up fight against disinformation campaigns during COVID-19 pandemic	Dedicated corner on fighting disinformation within the Commission's coronavirus response website[27] Tackling COVID-19 disinformation - Getting the facts right, JOIN(2020) 8 final
Internal coordination of myth busting efforts around narratives targeting the EU, via the management of the Network against Disinformation	Joint Communication Action Plan against Disinformation, JOIN (2018) 36 final

[24] https://www.disinfobservatory.org/.

[25] https://edmo.eu/.

[26] https://ec.europa.eu/digital-single-market/en/media-freedom-projects.

[27] https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_en.

Raising awareness and strengthening Europeans’ resilience against disinformation, via dissemination of educational audio-visual materials informing the public about the challenge of disinformation. This work is done in coordination with inter-institutional partners, including the Commission, the EEAS and the European Parliament	Communication on Tackling online disinformation: a European Approach, COM (2018) 236 final Joint Communication Action Plan against Disinformation, JOIN (2018) 36 final

5. Promoting EU common values and inclusive, open and resilient societies	
5.1 Radicalisation	
Measure	**Reference documents**
Imposing restrictive measures on ISIL (Da’esh) and Al-Qaeda, persons, entities associated with them and certain persons and entities with a view to combating terrorism	Council Decision (CFSP) 2016/1693 of 20 September 2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP Council Regulation (EU) 2016/1686 of 20 September 2016 imposing additional restrictive measures directed against ISIL (Da'esh) and Al-Qaeda and natural and legal persons, entities or bodies associated with them Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with the ISIL (Da'esh) and Al-Qaida organisations Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP) Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism
Coordinating voluntary measures of internet and social media companies tackling radicalisation within the EU Internet Forum	The European Agenda on Security, COM(2015) 185 final
Exchanging experience and developing best practices on prevention of radicalisation in particular through the Radicalisation Awareness Network (RAN)	The European Agenda on Security, COM(2015) 185 final Communication on supporting the prevention of radicalisation leading to violent extremism, COM(2016) 379 final Recommendation of High Level Commission Expert Group on Radicalisation (final report)[28]
The activities of the European Strategic Communications Network (a collaborative network of	

[28] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180613_final-report-radicalisation.pdf.

Member States set up to share analyses, good practice and ideas on the use of strategic communications in countering violent extremism) focused on supporting Member States to address a range of complex and inter-related communications challenges, including the influence of Jihadi networks, the extreme right wing and disinformation and hostile state actors	
Funding and trainings for the relevant projects under the Civil Society Empowerment Programme, an initiative under the EU Internet Forum	The European Agenda on Security, COM(2015) 185
Funding of counter-radicalisation projects in security research	Horizon 2020 Secure Societies Work Programme: Fighting Crime and Terrorism
5.2 Measures against illegal content online and hate speech	
Measure	**Reference documents**
Responsibility and due diligence by intermediaries in the management of their networks and systems	The European Agenda on Security, COM(2015) 185
Preventing and countering the spread of illegal hate speech online	Code of Conduct countering illegal hate speech online, 31 May 2016[29]
Strengthening cooperation within Europol's EU Internet Referral Unit on removing illegal content online	The European Agenda on Security, COM(2015) 185 final
Legislative measures on prevention, identification and swift removal of terrorist content online and robust safeguards to protect freedom of expression and information	Commission proposal for Regulation to prevent the dissemination of terrorist content online, COM (2018) 640 final Commission Recommendation on measures to effectively tackle illegal content online, C(2018) 1177 final The European Agenda on Security, COM(2015) 185 final Eighth progress report towards an effective and genuine Security Union, COM (2017) 354 final Communication on a Digital Single Market Strategy for Europe, COM(2015) 192 final Fifteenth Progress Report towards an effective and genuine Security Union, COM(2018) 470 final
Funding for projects aiming to remove illegal content online, incl. on methods to detect and analyse terrorist-related online contents and financing activities	Horizon 2020 Work Programme Secure Societies: Fighting Crime and Terrorism
5.3 Securing free and fair elections and protecting democratic processes	

[29] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

Measure	Reference documents
2018 Fundamental Rights Colloquium focused on democracy in the European Union, with dedicated sessions on secure electoral process and ensuring fair elections, pluralistic political debate, online and offline freedom of expression	
Supporting integrity of elections and electoral processes in the EU through the European Cooperation Network on elections, involving national authorities with competence for electoral matters and authorities in charge of monitoring and enforcing the rules on online activities relevant to the electoral context: sharing of expertise and best practices, including on threats, gaps and enforcement	Communication on securing free and fair European elections, COM(2018) 637 final Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final Guidance on the application of Union data protection law in the electoral Context, COM(2018) 638 final Documents relevant for the European elections network[30] Report on the 2019 elections to the European Parliament, COM(2020) 252 final
Conducting an exercise aimed at testing effectiveness of the EU's and MS response procedures and crisis plans in elections context	
Tackling cyber-enabled threats to elections in the framework of the NIS Cooperation Group and through workshops and exercises	NIS CG Publication 3/2018: Compendium on Cyber Security of Election Technology[31]

[30] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

[31] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645.

6. Protection of critical infrastructure	
Measure	**Reference documents**
Identifying and designating European critical infrastructure and common approach for assessing the need to improve its protection, including measures to facilitate the implementation of the EPCIP, expert groups at EU level, information-sharing and Critical Infrastructure Warning Information Network (CIWIN)	European Programme for Critical Infrastructure Protection, COM(2006) 786 final Directive 2008/114/EC on Critical Infrastructure Protection, OJ L 345, 23.12.2008, p. 75
Performing an evaluation of the Directive on Critical Infrastructure Protection taking into account hybrid threats aspects	Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, SWD(2019) 310 final
Increasing the critical infrastructure protection by funding research projects in different domains (transport, energy, health, finance, space, water, industrial facilities, communication, e-commerce system)	Horizon 2020 Secure Societies Work Programme: Infrastructure Protection
Identification of common tools, including indicators to improve protection and resilience of critical infrastructure against hybrid threats in the relevant sectors, covering technological, societal and media vulnerabilities	Developing vulnerability and detection indicators for hybrid threats, November 2018, JRC109791

7. Foreign direct investment screening

Measure	Reference documents
Launching of a cooperation mechanism to exchange information and to issue Member States' comments or Commission' opinions in relation to foreign direct investments likely to affect security or public order	Regulation 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, OJ L 79, 21.03.2019, p. 1 Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (FDI Screening Regulation), C(2020) 1981 final

8. Energy sector	
8.1 Security of energy supply	
Measure	**Reference documents**
Increasing security of energy supply in the EU by means of diversification of energy supply sources and routes	European Energy Security Strategy, COM(2014) 330 final A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, COM(2015) 80 final Fourth Report on the State of the Energy Union, COM(2019) 175 final
Preparedness for gas supply disruptions, including finalisation of risk assessments at regional and national levels (taking into account political, technological, commercial, social and natural risks, e.g. cyberattacks, sabotage, terrorism), regular Union-wide simulations by the European Network of Transmission System Operators for Gas (ENTSOG), preventive action plans and emergency plans and mitigating measures (e.g. solidarity principle)	Regulation 2017/1938 on security of gas supply, OJ L 280, 28.10.2017, p. 1
Guidelines for Member States on the implementation of solidarity and assistance, in particular on compensation	Commission Recommendation (EU) 2018/177 of 2 February 2018 on the elements to be included in the technical, legal and financial arrangements between Member States for the application of the solidarity mechanism under Article 13 of Regulation (EU) 2017/1938 of the European Parliament and of the Council concerning measures to safeguard the security of gas supply, OJ L 32, 6.2.2018, p. 52
Identification of vulnerabilities of critical supply chains for energy technologies and energy security in order to improve their resilience	
Rules for cooperation between Member States with a view to preventing, preparing for and managing electricity crises in a spirit of solidarity and transparency.	Regulation (EU) 2019/941 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 14.6.2019, p. 1 Commission Recommendation (EU) 2020/775 of 5 June 2020 on the key elements of the fair compensation and other key elements to be included in the technical, legal and financial arrangements between Member States for the application of the assistance mechanism, OJ L 184, 12.6.2020, p. 79
8.2 Nuclear safety and security	
Measure	**Reference documents**
Promoting safety and security standards to increase resilience of nuclear material and facilities, including the development of the rules on prevention of accidents and mitigation of accident consequences, cooperation and workshops with national authorities and regulators and monitoring of implementation of the outstanding safety improvements resulting from the EU stress tests	Nuclear Safety Directive 2009/71/Euratom, OJ L 172, 2.7.2009, p. 18, as amended by Directive 2014/87/Euratom, OJ L 219, 25.7.2014 Directive 2011/70/Euratom on the Spent Fuel and Radioactive Waste, OJ L 199, 2.8.2011, p. 48

following the Fukushima accident, etc.	Basic Safety Standards Directive 2013/59/Euratom, OJ L 13, 17.1.2014, p. 1. Commission Regulation (Euratom) No 302/2005 of 8 February 2005 on the application of Euratom safeguards, OJ L 54, 28.2.2005, p. 1 Commission Recommendation 2009/120/Euratom of 11 February 2009 on the implementation of a nuclear material accountancy and control system by operators of nuclear installations, OJ L 41, 12.2.2009, p. 17 Council Regulation (Euratom) No 1493/93 of 8 June 1993 on shipments of radioactive substances between Member States, OJ L 148, 19.6.1993, p. 1 Council Directive 2006/117/Euratom of 20 November 2006 on the supervision and control of shipments of radioactive waste and spent fuel between Member States and into and out of the Community, repealing Council Directive 92/3/Euratom, OJ L 337, 5.12.2006, p. 21 Commission Decision 2008/312/Euratom of 5 March 2008 establishing the standard document for the supervision and control of shipments of radioactive waste and spent fuel referred to in Council Directive 2006/117/Euratom, OJ L 107, 17.4.2008, p. 32 Commission Recommendation of 4 December (2008/956/Euratom) on criteria for the export of radioactive waste and spent fuel to third countries, OJ L 338, 17.12.2008, p. 69
8.3 Cybersecurity of energy networks	
Measure	**Reference documents**
Web-based platform: Incident and Threat Information Sharing EU Centre (ITIS)	Incident and Threat Information Sharing EU Centre[32]
Energy Expert Cyber Security Platform (EECSP) provides for a comprehensive energy sector strategy on cybersecurity in smart grid operations to reduce vulnerabilities and recommends actions for consideration by the Commission towards the development of energy cyber security strategy by analysis of respective cybersecurity challenges and existing policy papers	European Energy Security Strategy, COM (2014) 330 final A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, COM(2015) 80 final Best Available Techniques Reference Document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems, 2016[33]

[32] https://ec.europa.eu/jrc/en/scientific-tool/incident-and-threat-information-sharing-eu-centre-energy-sector-itis-euc.

Support to the European Energy Information Sharing and Analysis Centre (EE-ISAC) to share best practices, threat intelligence, incidents and other relevant information	
Setting up a dedicated energy work stream of the NIS Cooperation Group with an objective to monitor the status of the implementation of the Article 5 of the NIS Directive for the energy sector, analyse key findings, challenges and sectorial specificities	Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1
Measures to address real-time requirements, risk of cascading effects and combination of legacy systems with new technologies in the energy sector	Recommendation on cybersecurity in the energy sector, C (2019) 240 final Staff Working Document accompanying the document Commission Recommendation on cybersecurity in the energy sector, SWD (2019) 1240 final
Establishment of a network code on cybersecurity, in cooperation with the relevant associations of electricity network providers and regulators and monitoring of its implementation by the Member States	Regulation (EU) 2019/943 on the internal market for electricity, OJ L 158, 14.6.2019, p.54
Launching of a Thematic Network on Critical Energy Infrastructure Protection to foster collaboration among critical energy infrastructure operators in the energy sector (oil, gas, electricity)	
Development of the mmethodology for assessing seasonal and short-term adequacy developed by the EEuropean Network of Transmission System Operators for Electricity (ENTSO-E) and approved by the Agency for the Cooperation of Energy Regulators (ACER)	Short-term and Seasonal Adequacy Assessments Methodology, 6 January 2020[34]

[33] https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf.

[34] https://www.acer.europa.eu/en/Electricity/CLEAN_ENERGY_PACKAGE/Documents/Methodology%20for%20Short-term%20and%20Seasonal%20Adequacy%20Assessment_200106_submitted%20to%20ACER.pdf.

9. Transport sector	
9.1 Physical security of transport	
Measure	**Reference documents**
Constant improvement of the situational awareness on emerging security threats of hybrid nature in all areas of transport (civil aviation, maritime and land transport) through the EU Hybrid Fusion Cell's intelligence-based reporting, discussions with Member States authorities, industry and other stakeholders in expert groups, workshops and meetings	European Union Maritime Security Strategy, Council document 11205/14 Action Plan on the European Union Maritime Security Strategy, Council document15658/14, as revised by Council document 10494/18
Regular inspections on correct implementation of aviation and maritime security requirements and EU standards by the Member States, e.g. at airports, ports, air carriers and ships	Regulation (EC) 300/2008 on common rules in the field of aviation security, OJ L 97, 9.4.2008, p. 72 Commission Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, OJ L 299, 14.11.2015, p. 1 Regulation (EC) 725/2004 on enhancing ship and port facility security (ISPS Code), OJ L 129, 29.4.2004, p. 6 Directive (EC) 2005/65 on enhancing port security, OJ L 310, 25.11.2005, p. 28
Improving the security of rail transport by ensuring coordination at EU level, enhancing information sharing and raising the level of awareness, preparedness and capacity to respond to terrorist incidents, e.g. EU-wide risk-assessment, best practices on insider threats and on detection technologies suitable for railways	Further measures to improve passenger railway security, Annex to the Fifteenth Progress Report towards an effective and genuine Security Union, COM(2018) 470 final[35] Commission Decision of 29 June 2018 setting up the EU Rail Passenger Security Platform, OJ C 232, 3.07.2018, p.10
Improving security of road transport, incl. certification of safe and secure truck parking areas along the main European roads	EU Security Guidance for the European Commercial Road Freight Transport Sector, ROADSEC Security Toolkit[36]
Management and coordination of aviation network crisis, incl. security incidents and cyberattacks, in particular through the European Aviation Crisis Coordination Cell (ECCC)	Regulation 2019/123 on Air Traffic Network Functions, OJ L 28, 31.1.2019, p. 1
Regular security risk assessments in the aviation sector, incl. common methodology to identify threats and to support the development of effective and proportionate mitigation measures	Conflict Zones Information Bulletin by EASA, since March 2017[37]
Supporting the Member States in countering threats by unmanned aircraft systems (UAS),	Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the

[35] https://ec.europa.eu/transport/sites/transport/files/com20180470-annex.pdf.

[36] https://ec.europa.eu/transport/themes/security/land_security/road-security-toolkit_en.

[37] https://www.easa.europa.eu/easa-and-you/air-operations/information-on-conflict-zones.

notably by providing for the registration of drone operators, the mandatory remote identification of drones, and by contributing to the greater preparedness of airports	rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019, p. 45 Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019, p. 1 Chair's Statement on the outcome of the High-Level International Conference and subsequent EU-internal meeting on countering the threats posed by unmanned aircraft systems (UAS), Brussels, 18 October 2019[38] EASA Counter Drones (C-UAS) proposed action plan, issue 2, 5 July 2019[39]
Addressing threats to maritime security through cross-sectorial cooperation, including between civilian and military actors to protect maritime critical infrastructure, global supply chain, maritime trade and maritime natural and energy resources	European Union Maritime Security Strategy (EUMSS), Council document 11205/14 Action Plan on EUMSS, Council document15658/14, as revised by Council document 10494/18 Review of the Common Information Sharing Environment (CISE) for the maritime domain: 2014 – 2019, SWD (2019) 322 final Study on Security Measures for Ro-ro Ferries, December 2017 Study on Cruise Ship Security, June 2016
Analysis of developments and trends in maritime security, covering also piracy and maritime disputes that could disrupt shipping and trade routes	
Launching the transitional phase of the Common Information Sharing Environment (CISE) aimed at bringing the network into day-to-day operations	CISE Transitional Phase: Activities and CISE Transitional Phase: Governance Structure [40]
Further contribute to EU maritime situational awareness including through maritime surveillance (MARSUR)	European Union Maritime Security Strategy (EUMSS), Council document 11205/14 Action Plan on EUMSS, Council document15658/14, as revised by Council document 10494/18

[38] https://ec.europa.eu/transport/sites/transport/files/2019-10-17-chair-statement.pdf.

[39] https://www.easa.europa.eu/newsroom-and-events/news/one-step-closer-harmonised-rules-safe-drones-operation-europe; https://www.eurocontrol.int/sites/default/files/2019-10/2-easa-florin.pdf.

[40] http://www.emsa.europa.eu/cise/transitional-phase.html.

9.2 Cybersecurity of the transport sector	
Measure	**Reference documents**
Improving integration of cybersecurity dimension in the maritime domain in terms of capabilities, research and technology and industry, building on civil-military coordination and synergies with EU cyber policies, in line with the NIS Directive	European Union Maritime Security Strategy, Council document 11205/14 Action Plan on the European Union Maritime Security Strategy , Council document15658/14, as revised by Council document 10494/18 Reports on implementation of the Action Plan on the European Union Maritime Security Strategy [41] Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions in order to identify commonalities and ways to enhance interoperability and cooperation in this field across EU, 30 March 2017[42]
Implementation of NIS Directive in the transport sector (including work with the NIS Cooperation Group involving representatives of the transport sector) and promoting cyber skills and information sharing (all transport modes)	Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1
Strengthening port cybersecurity, e.g. workshop organised by the EU Cybersecurity Agency ENISA and EMSA (November 2019)	Port Cybersecurity - Good practices for cybersecurity in the maritime sector[43]
Highlighting to stakeholders and Member States the cybersecurity-related obligations under existing EU maritime security legislation (e.g. “computer systems and networks” are listed as part of the assets and infrastructure that need to be protected)	Regulation (EC) No 725/2004 on enhancing ship and port facility security, OJ L 129, 29.4.2004, p. 6 Directive 2005/65/EC on enhancing port security, OJ L 310, 25.11.2005, p. 28
Addressing emerging threats to submarine piping, energy transfer, fibre optic and traditional communications cabling from interference outside national waters	European Union Maritime Security Strategy, Council document 11205/14 In 2018, the Commission and EEAS completed the civil-military Strategic Research Agenda (MRA) under EUMSS AP[44]
Recommendations of good practices to support security managers and professionals in the transport sector to better identify, assess and mitigate cyber security risks, covering maritime security in general, including transport, critical infrastructure, surveillance systems, etc.	European Union Maritime Security Strategy, Council document 11205/14 Action Plan on the European Union Maritime Security Strategy, Council document 15658/14, as revised by Council document 10494/18
Implementation of the roadmap on aviation cybersecurity and preparation of EU Cybersecurity	Aviation Strategy for Europe, COM(2015) 598 final

[41] https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en.

[42] https://op.europa.eu/en/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1.

[43] https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

[44] https://www.statewatch.org/media/documents/news/2018/feb/eu-jrc-civil-military-research-agenda-maritime-security-18-12-17.pdf.

Strategy in aviation by the European Strategic Coordination Platform on Cybersecurity of EASA	Regulation (EU) 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, OJ L 212, 22.8.2018, p. 1 EASA's EU Cybersecurity Strategy in aviation[45] Roadmap on cybersecurity in aviation – EASA MB 03/2015 WP14 – Cybersecurity Roadmap 14 and 15 December 2015[46]
Supporting EASA and EUROCONTROL to help these entities and their stakeholders dealing with cyber threats by information sharing, threat analysis and standardisation programme, incl. European Centre for Cyber Security in Aviation (ECCSA) and Computer Emergency Response Team on Aviation	
Conducting a gap analysis of existing cybersecurity rules in aviation with proposals for integrating the results into the EU law	EASA's Notice of Proposed Amendment 2019-07 on the Management of information security risks EASA Rulemaking task RMT.0720[47]
Establishment of the Task Force on Cybersecurity in Single European Sky Air Traffic Management Research (SESAR) Joint Undertaking (incl. with military inputs from EDA)	
Update of EU Aviation Security legislation to address cybersecurity through the incorporation of requirements in the areas of training, security awareness, and background checks on staff having critical roles in information technology systems	Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures, OJ L 246, 26.9.2019, p. 15

[45] https://www.easa.europa.eu/domains/cyber-security/main-easa-activities.

[46] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[47] https://www.easa.europa.eu/rulemaking-tasks/rmt0720.

10. Border control and supply chain security

Measure	Reference documents
Increasing maritime situational awareness and supporting coherent and cost-efficient action through closer cooperation between coast guard functions of the relevant EU agencies (EFCA, EMSA and Frontex) and with national authorities, in particular on information sharing, surveillance and communication services, capacity building, risk analysis and capacity sharing and through the European Coast Guard Functions Forum (ECGFF)	Regulation 2016/1624 on the European Border and Coast Guard, OJ L 251, 16.9.2016, p. 1 European Union Maritime Security Strategy, Council document 11205/14 Action Plan on the European Union Maritime Security Strategy, Council document15658/14, as revised by Council document 10494/18
Significant upgrade of advance cargo information (incl. IT systems) and customs risk management system with a view to early detecting and mitigating serious security and safety risks, covering integrity of international supply chains, threats to critical infrastructure resulting from imports, e.g. at sea-port facilities, airports or land borders	European Union Customs Risk Management Strategy and Action Plan, COM (2014) 527 final Second progress report on EU Customs Risk Management Strategy and Action Plan, COM(2018) 549 final CBRN Action Plan, COM(2017) 610 final
Programming and implementation of research and innovation for border management and security (border surveillance and border checks), customs security and supply chains security building future capabilities to support Integrated Border Management, EU Maritime Security Strategy and EU Customs Risk Management Strategy and Action Plan	Horizon 2020 Secure Societies Work Programme: Border and External Security Horizon Europe Cluster 3 Strategic Orientations

11. Space sector	
Measure	**Reference documents**
Increasing protection of both ground and space segments of the critical space infrastructure: Galileo, Copernicus, Space Surveillance and Tracking (SST) and GovSatCom, including both physical protection and data security measures	Commission Communication A Space Strategy for Europe, COM(2016) 705 Decision 541/2014/EU establishing a Framework for Space Surveillance and Tracking Support, OJ L 158, 27.5.2014, p. 227 Space Situational Awareness Data Policy, Council document 14698/12 Council Decision 2014/496/CFSP on aspects of the deployment, operation and use of the European GNSS, OJ L 219, 25.7.2014, p. 52 Commission Proposal for EU Space Programme, COM 2018 (447) final Council's recommendations on security aspects of the Space Situational Awareness data policy
Development of the next generation of Governmental Satellite Communications (GovSatCom), providing guaranteed and secured access to satellite communications to EU and MS missions and operations but also key infrastructure	Commission Proposal for EU Space Programme, COM 2018 (447) final
Provision of satellite images of Copernicus for security-related activities on the ground, e.g. border surveillance, crisis prevention and recovery, monitoring and assessment of vulnerabilities of critical infrastructure	Regulation (EU) No 377/2014 establishing the Copernicus Programme, OJ L 122, 24.4.2014, p. 44
Strengthening capacity to counter hostile intelligence and communication campaigns by introducing Galileo in critical infrastructure for time synchronisation	Council Decision 2014/496/CFSP on aspects of the deployment, operation and use of the European GNSS, OJ L 219, 25.7.2014, p. 52
Use of space-enabled services to counter hybrid threats through increasing resilience of critical infrastructure (e.g. energy grids, telecommunications networks, financial transactions)	Commission Proposal for EU Space Programme, COM 2018 (447) final

12. Defence capabilities, including cyber defence	
Measure	**Reference documents**
Identification of relevant key defence capability areas for the EU Collaborative projects on capability development, Cyber Education, Training and Exercises, and Research & Technology	Capability Development Plan EDA's Strategic Context Cases
Strengthening defence capabilities by means of financing of relevant research and capabilities development projects, including for cyber defence	European Defence Action Plan, COM(2016) 950 final Commission Financing Decision on the Preparatory Action on Defence Research, C(2017) 2262 final Regulation (EU) 2018/1092 on the European Defence Industrial Development Programme, OJ L 200, 7.8.2018, p. 30 Proposal for Regulation on the European Defence Fund, COM(2018) 476 final European Defence Industrial Development Programme work programme[48] European Defence Industrial Development Programme 2019-2020 calls[49] European Defence Industrial Development Programme award decisions: Commission Implementing Decision of 15 June 2020, C(2020) 4068 final; Commission Implementing Decision of 15 June 2020, C(2020) 4067 final
Launching Cyber Education, Training, Exercises and Evaluation (ETEE) platform	EU Cyber Defence Policy Framework, Council document ST 14413/18
PESCO projects on cyber defence[50]	Cyber Rapid Response Teams and Mutual Assistance in Cyber Security Cyber Threats and Incident Response Information Sharing Platform Strategic Context Case on the 2018 EU Capability Development Priority Enabling Capabilities for Cyber Responsive Operations

[48] https://ec.europa.eu/docsroom/documents/34515.

[49] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-search.

[50] https://pesco.europa.eu/.

Identification of common capability and research shortfalls and collaborative opportunities to address energy security challenges including energy efficiency, buildings performance and renewable energy solutions in the defence sector and the protection of defence-related critical energy infrastructure	Guidance Document: CF SEDSS II Results and Recommendations for Sustainable Energy in the Defence and Security Sector (issued July 2019) PCEI Conceptual paper prepared by the Protection of Critical Energy Infrastructure Experts Group of EDA (October 2017) Situational Awareness System for Systemic Decision Support for Defence Energy Infrastructures Information sheet

13. Military aspects of the Common Security and Defence Policy

Measures	Reference documents
Development of conceptual tools strengthening EU-led military operations	EU concept for EU-led Military Operations and Missions EU Concept on Cyber Defence for EU-led Military Operations and Missions EU Concept for CBRN EOD in EU-led Military Operations EU Concept on Consequence Management after CBRN Incident for EU-led Military Operations and Missions Standard Operational Procedure (SOP) on countering hybrid threats in CSDP Military Operations and Missions

14. Protecting public health and food security	
14.1. Public health, incl. healthcare infrastructure	
Measure	**Reference documents**
Coordination of preparedness for serious cross-border threats to health in the framework of the Health Security Committee, linking Member States, EU agencies and Scientific Committees through the Early Warning and Response System	Decision 1082/2013 on serious cross-border threats to health, OJ L 293, 5.11.2013, p. 1 Commission Decision on establishment of Scientific Committees in the field of public health, consumer safety and the environment, C(2015)5383/F1
Setting up of a network Global Research Collaboration for Infectious Disease Preparedness (GloPID-R) for coordinated research response within 48 hours of any significant outbreak	
Support to the Member States through training, simulation exercises, exchange of experience guidelines, financing Joint Actions and R&D projects and targeted communication campaigns	Report on the tabletop exercise on Hybrid threats involving public health and civil protection/security authorities Luxembourg 30-31 January 2018[51] Regulation (EU) No 282/2014 on the establishment of a third Programme for the Union's action in the field of health (2014-2020) and repealing Decision No 1350/2007/EC, OJ L 86, 21.3.2014, p. 1 Proposal for a Regulation of the European Parliament and of the Council on the establishment of a Programme for the Union's action in the field of health –for the period 2021-2027 and repealing Regulation (EU) No 282/2014 ("EU4Health Programme"), COM(2020) 405 final Proposal for a Regulation on the establishment of a Programme for the Union's action in the field of health –for the period 2021-2027, COM(2020) 405 final Commission Communication and proposal for Council recommendation on Strengthened Cooperation against Vaccine Preventable Diseases, COM(2018) 244 final Council Recommendation on strengthened cooperation against vaccine-preventable diseases, OJ C 466, 28.12.2018, p. 1
Research funding for the improvement of physical and cyber security of hospitals as well as networking activities of health first responders	Horizon 2020 Secure Societies Work Programme: Disaster Resilient Societies and Infrastructure Protection

[51] https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/2018_hybridthreatsexercise_en.pdf.

Analysis of possible hybrid threats during the COVID-19 pandemic	Geopolitical and possible Hybrid Threat activities related to the COVID-19 pandemic: An updated analysis based on information up to 7/4/2020, JRC120699 Geopolitical and possible Hybrid Threat activities related to the COVID-19 pandemic: An updated analysis based on information up to 26/4/2020, JRC120701 Hybrid Fusion Cell intelligence assessments on information and cyber threats related to COVID-19, ref. EEAS (2020) 10146, EEAS (2020) 10147, EEAS (2020) 10154
Building strategic stockpiles at EU level (under rescEU) of essential medical countermeasures (vaccines and therapeutics), personal protective equipment, medical equipment and laboratory supplies for situations of serious cross-border threats to health	Commission Implementing Decision (EU) 2020/414 of 19 March 2020 amending Implementing Decision (EU) 2019/570 as regards medical stockpiling rescEU capacities, OJ L 82I , 19.3.2020, p. 1
14.2. Food security	
Measure	**Reference documents**
Monitoring of health risks posed by contaminated food through exchange of risk analysis information between competent authorities under the Rapid Alert System for Food and Feed (RASFF), Early Warning and Response System (EWRS) and Common Risk Management System (CRMS) for customs	Commission Implementing Decision (EU) establishing a general plan for crisis management in the field of the safety of food and feed, C(2019) 1064
Collaboration with the European Food Safety Authority and the European Centre for Disease Prevention and Control to adapt to advanced scientific investigation techniques with a view of more precise identification and sourcing health threats and consequently rapid management of food safety outbreaks	Commission Implementing Decision (EU) establishing a general plan for crisis management in the field of the safety of food and feed, C(2019) 1064
Improving surveillance and eradication as well as containment measures for high risk plants and pests	Regulation (EU) 2016/2031 on Plant Health Law, OJ L 317, 23.11.2016, p. 4
Supporting broader use of new technologies for animal health activities, in terms of surveillance of pathogens, electronic identification and registration of animals. Provide for better early detection and control of animal diseases, including emerging diseases linked to climate change and help to reduce the occurrence and effects of animal epidemics	Regulation 2016/429 on Animal Health Law, OJ L 84, 31.3.2016

15. Civil protection

Measure	Reference documents
Improving resilience to hybrid threats within existing preparedness and coordination mechanisms in civil protection	Preparing for mass burn casualty incidents, SWD(2020) 3 final Workshop on mass casualties from the deliberate release of opioids, 21-22 January 2020[52]
Funding of projects under the Union Civil Protection Mechanism to increase urban resilience and on critical infrastructure	Annual UCPM calls for prevention and preparedness project (single country and multi-country)[53]
Stepping up disaster prevention, preparedness and response capacities through the new Union Civil Protection Mechanism, with specialised task teams on rescEU capacities, e.g. medical and CBRN	Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism Proposal for a Decision of the European Parliament and of the Council amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism, COM(2020) 220 Commission Implementing Decision (EU) 2019/570 of 8 April 2019 laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council as regards rescEU capacities and amending Commission Implementing Decision 2014/762/EU, OJ L 99, 10.4.2019, p. 41
European Medical Corps as part of the Union Civil Protection Mechanism avails medical capacities to be deployed in case of acute health emergencies	
Establishing necessary capacities, including financing, to respond to low probability risks with a high impact (under rescEU): Medevac, EMT-3 and strategic stockpiling	Commission Implementing Decision (EU) 2018/142 amending Implementing Decision 2014/762/EU laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism Commission Implementing Decision (EU) 2020/414 of 19 March 2020 amending Implementing Decision (EU) 2019/570 as regards medical stockpiling rescEU capacities, OJ L 82I , 19.3.2020, p. 1 Commission Implementing Decision (EU) 2020/452 of 26 March 2020 amending Implementing Decision (EU) 2019/570 as regards capacities

[52] https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/ev_20200121_mi_en.pdf.

[53] https://ec.europa.eu/echo/funding-evaluations/financing-civil-protection-europe/prevention-and-preparedness-projects-civil-protection_en.

	established to respond to low probability risks with a high impact, OJ L 94I , 27.3.2020, p. 1

16. Addressing Chemical, Biological, Radiological and Nuclear related risks

Measure	**Reference documents**
Comprehensive training on radiation and nuclear detection techniques, trends and new challenges for customs experts from the Member States	
Radioactive source control measures, e.g. record keeping and security of high-activity sources	Directive 2013/59/Euratom on basic safety standards for protection against the dangers arising from exposure to ionising radiation, OJ L 13, 17.1.2014, p. 1 Council Regulation (Euratom) No 1493/93 of 8 June 1993 on shipments of radioactive substances between Member States, OJ L 148, 19.6.1993, p. 1 Commission Regulation (Euratom) No 302/2005 of 8 February 2005 on the application of Euratom safeguards, OJ L 54, 28.2.2005, p. 1 Commission Recommendation 2009/120/Euratom of 11 February 2009 on the implementation of a nuclear material accountancy and control system by operators of nuclear installations, OJ L 41, 12.2.2009, p. 17
Setting up the EU autonomous restrictive measures regime against the proliferation and use of chemical weapons	Council Decision (CFSP) 2018/1544 concerning restrictive measures against the proliferation and use of chemical weapons, OJ L 259, 16.10.2018, p. 25 Council Regulation (EU) 2018/1542 concerning restrictive measures against the proliferation and use of chemical weapons, OJ L 259, 16.10.2018, p. 12
Reducing accessibility of chemical substances posing particular threat: classified list of more than 20 chemical substances of concern, cooperation with chemical supply chain (incl. producers of precursors) and with equipment manufacturers on detection capabilities as well as with online platforms on suspicious transactions	CBRN Action Plan, COM(2017) 610 final Report on gap analysis of CBRN materials and agents, June 2018
Funding to practitioners, research organisations and industry (including SMEs) for targeted security research on CBRN as well as networking activities	Horizon 2020 Secure Societies Work Programme: Disaster Resilient Societies and General Matters

17. Cybersecurity	
Measure	**Reference documents**
Setting out a framework for a coordinated response to large-scale cybersecurity incidents and crises under the Blueprint Recommendation through the Cyber Crises Liaison Organisation Network (CyCLONe), composed of national Cyber Crises Liaison Organisations (CyCLOs), supported by the EU Cybersecurity Agency ENISA	Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017, p. 36
Exercises in cybersecurity at the operational level of Blueprint	After Action Report of Blue OLEx 2019 cybersecurity exercise (Paris, July 2019)
Increasing the security of 5G networks	Commission Recommendation on the Cybersecurity of 5G networks, C(2019) 2335 final EU coordinated risk assessment of cybersecurity of 5G network (Report of NIS Cooperation Group), 9 October 2019[54] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures (Report of NIS Cooperation Group), 29 January 2020[55] Commission Communication on 'Secure 5G deployment in the EU- Implementing the EU toolbox, COM 2020 (50) final Report on the implementation of the 5G Cybersecurity Toolbox (Report of NIS Cooperation Group), July 2020[56]
Establishing cyber threat intelligence fusion cell CERT-EU and network of Computer Security Incident Response Teams (CSIRTs) to monitor landscape and prepare cyber threat assessment products related to critical sectors	Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1
Establishing cross agencies cooperation on cybersecurity to develop synergies and provision of expertise, operational and technical support to the EU and the Member States	Memorandum of Understanding between ENISA, CERT-EU, EDA and EC3 of Europol, May 2018[57]
Addressing cybersecurity risks throughout a broad range of essential service providers in the fields of energy, transport, water, healthcare, banking, financial and digital infrastructure sectors, in line with the NIS Directive	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)1 final Joint Communication on Resilience, Deterrence and Defence: Building strong

[54] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[55] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[56] https://ec.europa.eu/digital-single-market/news-redirect/683481.

[57] https://www.eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf.

	cybersecurity for the EU, JOIN(2017) 450 final The European Agenda on Security, COM(2015) 185 final Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1 Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017, p. 36 Recommendation on cybersecurity in the energy sector, C(2019) 2400 final
Establishment of a Cooperation Group under the NIS Directive as a forum for strategic cooperation both on horizontal cybersecurity issues and thematic work streams, e.g. on Blueprint Recommendation	Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1
Stimulating development of R&D technologies in cybersecurity through contractual Public Private Partnership with the European Cybersecurity Organisation (ECSO)	Digital Single Market Strategy, COM(2015) 192 final Commission Decision on signing cPPP, C(2016) 4400 Monitoring report on cPPP[58]
Stimulating development and deployment of cybersecurity solutions through the proposal to establish Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres, including four pilot projects under H2020	Proposal for Regulation to establish a Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres, COM(2018) 630 final
Strengthening the mandate of the European Union Agency for Cybersecurity ENISA: better contribution to EU and Member States activities in the areas of operational cooperation, crisis management, capability development and awareness raising and thereby strengthening the resilience of the EU to cyber – and hybrid - attacks	Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity in Europe, JOIN(2017) 450 final Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15
Development of the EU cybersecurity certification framework for information and communications technology products and services, incl. 2019 full scale pilot project for definition and testing within a European scheme for cybersecurity certification of Industrial Automation Control System Components (IACS)	Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity in Europe, JOIN(2017) 450 final Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act) OJ L 151, 7.6.2019, p. 15

[58] https://www.ecs-org.eu/documents/publications/5db82678564e8.pdf.

Development of the cyber diplomacy toolbox contributing to conflict prevention, mitigation of cybersecurity threats and greater stability in international relations	Joint Communication on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 7.2.2013 JOIN (2103) 01 final 2015 Council Conclusions on Cyber Diplomacy[59] 2017 Joint Communication on A Strategic Approach to Resilience in the EU's external action 7.6.2107 JOIN(2017) 21 final Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, Council document 9916/17 Implementing guidelines for cyber diplomacy toolbox, October 2017 – (13007/17) Council conclusions on EU External Cyber Capacity Building Guidelines, (10496/18)
Establishment of the framework for imposing sanctions in case of cyber-attacks threatening the Union or its Member States	Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I , 17.5.2019, p. 13 Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I , 17.5.2019, p. 1

[59] http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

18. Financial transactions

Measure	Reference documents
Promotion and facilitation of cyber threats information sharing platforms and networks among financial market players	FinTech Action plan: For a more competitive and innovative European financial sector, COM(2018) 109 final
Participating in the European Central Bank's European Cyber Resilience Board for pan-European financial infrastructures (ECRB) sub-working group on information sharing arrangements, gathering private sector participants and authorities (both EU and national level) and working on building blocks to enable trusted network for information sharing among pan-European financial infrastructures	
Enhancing security in payment transactions and strong customer authentication with the aim to reduce fraud, especially in online payments	Payment Services Directive 2015/2366, OJ L 337, 23.12.2015, p. 35 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ L 69, 13.03.2018, p. 23
Addressing fragmentation in relation to the scope, granularity and specificity of cybersecurity related provisions across the EU financial services legislation	Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements in the European Union (EU) financial sector, JC 2019 26, 10 April 2019 Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector, JC 2019 25, 10 April 2019
Strengthening the digital operational resilience of the EU financial sector entities	Inception Impact Assessment, Regulation on Digital Operational Resilience for the Financial Sectors Consultation document: A potential initiative on the digital operational resilience in the area of financial services
Combating money laundering and the financing of terrorism	Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (4th), OJ L 141, 5.6.2015, p. 73 Commission Communication "Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework", COM (2019) 360 final

	Supranational Risk Assessment report and annex, COM/2019/370 final, SWD(2019) 650 final Report assessing the framework for cooperation between Financial Intelligence Units, COM (2019) 371 final Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts, COM (2019) 372 final Report on the assessment of recent alleged money laundering cases involving EU credit institutions, COM (2019) 373 final Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, COM (2020) 2800 final Commission Staff Working Document "Methodology for identifying high-risk third countries under Directive (EU) 2015/849", SWD (2020) 99 final Commission Delegated Regulation (EU) 2020/855 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding the Bahamas, Barbados, Botswana, Cambodia, Ghana, Jamaica, Mauritius, Mongolia, Myanmar/Burma, Nicaragua, Panama and Zimbabwe to the table in point I of the Annex and deleting Bosnia-Herzegovina, Ethiopia, Guyana, Lao People's Democratic Republic, Sri Lanka and Tunisia from this table, OJ L 195, 19.06.2020, p.1
Controlling cash entering or leaving the European Union	Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 OJ L 284, 12.11.2018, p. 6
Controlling the introduction and the import of cultural goods	Regulation (EU) 2019/880 on the introduction and the import of cultural goods OJ L 151, 7.6.2019, p. 1
Facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, including money laundering and the financing of terrorism	Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L 186, 11.7.2019, p. 122
Harmonising criminal offences and sanctions for money laundering	Directive (EU) 2018/1673 on combating money laundering by criminal law, OJ L 284, 12.11.2018, p. 22

Targeting hybrid threats financing through measures against crime and terrorist financing, e.g. traceability of funds transfers, monitoring of virtual currency exchange platforms, transparency of pre-paid instruments, safeguards against illicit cash movements and trade in cultural goods, including cooperation with and among national Financial Intelligence Units and with law enforcement authorities	Directive (EU) 2018/843, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing OJ L 156, 19.6.2018, p. 43

19. Cooperation with third countries	
19.1. EU's neighbourhood	
Measure	**Reference documents**
Hybrid risk surveys in the EU's neighbourhood	Joint Communication on a Strategic Approach to Resilience in the EU's external action, JOIN(2017) 21 final
Exchange of operational and strategic expertise with enlargement countries, Eastern Partnership and Southern Neighbourhood on e.g. combating organised crime, counter terrorism, irregular migration, trafficking of small arms	The European Agenda on Security, COM(2015) 185 final Joint Communication on the review of the European Neighbourhood Policy, JOIN(2015) 50 final Eastern Partnership - 20 Deliverables for 2020 Focusing on key priorities and tangible results - SWD(2017) 300 final Eastern Partnership policy beyond 2020 - Reinforcing Resilience - an Eastern Partnership that delivers for all, JOIN(2020) 7 final A credible enlargement perspective for an enhanced EU engagement with the Western Balkans, COM(2018) 65 final EU-Western Balkans Sofia Declaration and Sofia Priority agency, 17 May 2018[60]Commission Communication "Enhancing the accession process – A credible EU perspective for the Western Balkans", COM(2020) 57 final The Zagreb Declaration, 6 May 2020[61] Joint EEAS-COM non-paper: Update on the implementation of the European Neighbourhood Policy security dimension (July 2018 – June 2019)[62]
Capacity building through external financing instruments, for example: • EU-funded project aiming at improving cyber resilience in the Eastern Partnership countries with two components: cybersecurity and cybercrime; • Providing cybersecurity capacity building assistance to Ukraine, by reinforcing	Joint Communication on the review of the European Neighbourhood Policy, JOIN(2015) 50 final Communication from the Commission - A credible enlargement perspective for an enhanced EU engagement with the Western Balkans - COM(2018) 65

[60] https://www.consilium.europa.eu/media/34776/sofia-declaration_en.pdf.

[61] https://www.consilium.europa.eu/media/43776/zagreb-declaration-en-06052020.pdf.

[62] Ares(2019)3954880 - 21/06/2019.

cybersecurity in elections, delivering trainings, seminars and creating a platform for Public Private Partnership; • Regional programme aiming at building up functioning and accountable institutions in the Western Balkans to strengthen the region's cyber resilience.	final Eastern Partnership policy beyond 2020 - Reinforcing Resilience - an Eastern Partnership that delivers for all, JOIN(2020) 7 final The New European Consensus on Development "Our World, Our Dignity, Our Future", Joint Statement by the Council and the Representatives of the Governments of the Member States meeting within the Council, the European Parliament and the European Commission, 7 June 2017[63] Joint Communication on capacity building in support of security and development enabling partners to prevent and manage crises, JOIN(2015) 17 final Regulation (EU) 230/2014 establishing an instrument contributing to stability and peace, OJ L 77, 15.3.2014, p. 1 Regulation (EU) No 231/2014 of 11 March 2014 establishing an Instrument for Pre-accession Assistance (IPA II), OJ L 77, 15.3.2004, p. 11 Regulation (EU) No 232/2014 of 11 March 2014 establishing a European Neighbourhood Instrument, OJ L 77, 15.3.2004, p. 27
Developing closer internal-external contacts between the EU and the network set up in the framework of the EU CBRN risk mitigation Centres of Excellence (EU CBRN CoE) initiative, including in the EU neighbourhood	CBRN Action Plan, COM(2017) 610 final
Increasing civil protection by means of training and exercises under the regional programmes of Prevention, Preparedness and Response to natural and man-made disasters (PPRD) with close links to the EU CBRN Centres of Excellence initiative	
19.2. International and bilateral cooperation beyond the EU's neighbourhood	
Measure	**Reference documents**
Structural cooperation between the Rapid Alert System and G7 Rapid Response Mechanism.	Joint Letter of EEAS StratCom and RRM Canada on the structured cooperation between the RAS and the RRM
Establishment and joining to the Canberra Group on Disinformation	Terms of Reference of the Canberra Group on Disinformation
Cooperation with US, Hedayah Centre of Excellence on Countering Violent Extremism, Global Community Engagements and Resilience Fund with partner countries in the Middle East, North Africa, Sahel, Horn of Africa, WB and across Asia to facilitate innovative preventing and	Regulation (EU) 230/2014 establishing an instrument contributing to stability and peace, OJ L 77, 15.3.2014, p. 1

[63] https://ec.europa.eu/international-partnerships/system/files/european-consensus-on-development-final-20170626_en.pdf.

countering violent extremism projects in collaboration with local communities, to strengthen condition conductive to development and build resilience towards violent extremism	
External engagement and outreach, capacity building, prevention and fostering resilience to address underlying economic, political and societal factors of radicalisation and extremist content, incl. engagement with partners from the UN as well as other multilateral fora (GCTF and its inspired institutions) on preventing and countering violent extremism	Regulation (EU) 230/2014 establishing an instrument contributing to stability and peace, OJ L 77, 15.3.2014, p. 1
Cooperation with G7 and G20 countries (as well as with online platforms) to remove illegal content online	G7 2019 Ministerial Meeting Outcome Document on combating the use of Internet for terrorist and violent extremist purposes[64] G7 2019 Charter for a free, safer and open Internet[65] G20 2019 Osaka Leaders' statement on preventing exploitation of the internet for terrorism and violent extremism conducive to terrorism[66]
EU-US expert-level dialogue on resilience of electoral systems, November 2019	
Framework for the cooperation with third countries in critical infrastructure protection	European Programme for Critical Infrastructure Protection, COM(2006) 786 final
Developing cooperation with the International Atomic Energy Agency and the US government in the Border Monitoring Working Group (currently chaired by the Commission) on nuclear security capacity building	
Promoting international cooperation on emergency preparedness and response in nuclear safety and security	Nuclear Safety Directive 2009/71/Euratom, OJ L 172, 2.7.2009, p. 18, as amended by Directive 2014/87/Euratom, OJ L 219, 25.7.2014 Basic Safety Standards Directive 2013/59/Euratom, OJ L 13, 17.1.2014, p. 1. Council Decision 87/600/Euratom of 14 December 1987 on Community arrangements for the early exchange of information in the event of a radiological emergency (ECURIE), OJ L 371, 30.12.1987, p. 76
Strengthening an international cooperation on cybersecurity in air transport at the level of International Civil Aviation Organisation (ICAO), incl. funding project to strengthen the capacity of partner countries to protect and respond effectively to cyber threats against civil aviation assets, with focus on sharing expertise, mentoring, training and coaching activities, including a series of activities leading to the implementation of Annex XVII on security standards for civil aviation to Chicago Convention	United Nations Security Council Resolution 2309/2016 on terrorist threats to civil aviation[67] International Civil Aviation Organization, Convention on International Civil Aviation (Chicago Convention), Annex 17 on Security Standards and Annex 9 on Facilitation

[64] https://www.elysee.fr/admin/upload/default/0001/04/287b5bb9a30155452ff7762a9131301284ff6417.pdf.

[65] https://www.entreprises.gouv.fr/files/files/directions_services/numerique/Charter-for-a-free-open-and-safe-Internet.pdf.

[66] https://www.diplomatie.gouv.fr/IMG/pdf/2._g20_osaka_statement_on_preventing_terrorist_and_vetc_en_cle88a229.pdf.

[67] https://www.un.org/press/en/2016/sc12529.doc.htm.

	International Civil Aviation Organization, Resolution A40-12/3: Declaration on aviation security[68] International Civil Aviation Organization, Doc 10118, Global Aviation Security Plan, First Edition 2017[69] Commission Implementing Regulation 2019/103 on aviation security, OJ L 21, 24.1.2019, p. 13 Regulation (EU) 230/2014 establishing an instrument contributing to stability and peace, OJ L 77, 15.3.2014, p. 1
International cooperation on cybersecurity in maritime transport in the framework of the International Maritime Organization (IMO)	International Maritime Organisation, Guidelines on Maritime Cyber risk Management, 5 July 2017[70] International Maritime Organisation, Resolution MSC.428(98), Maritime cyber risk management in safety management systems, 16 June 2017[71]
Multilateral cooperation in the health sector at the level of World Health Organisation and the European Burns Association, including implementation of International Health Regulations aiming to prevent and respond to acute public, cross-border health risks worldwide	International Health Regulations[72] Strengthened International Health Regulations and Preparedness in the EU - Joint Action [SHARP JA] [848096][73]
Bilateral cooperation with the US Centres for Disease Control and Prevention and FBI on joint criminal-epidemiological investigations	
Support of core activities of the Organisation for the Prohibition of Chemical Weapons	Council Decision (CFSP) 2019/538 from 1 April 2019
International cooperation and capacity building in third countries in relation to CBRN risks, including through a number of large scale regional capacity building projects funded under the EU CBRN Centres of Excellence initiative, for instance in the field of emergency and medical response, forensics, bio safety and bio security, export control	CBRN Action Plan, COM(2017) 610 final
Participation in an open-ended working group at the UN level in the context of ICT developments in international security, Group of Governmental Experts to advance responsible	

[68] https://www.icao.int/Meetings/a40/Documents/WP/wp_596_add1_en.pdf.

[69] https://www.icao.int/Security/Documents/GLOBAL%20AVIATION%20SECURITY%20PLAN%20EN.pdf.

[70] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

[71] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf.

[72] https://www.who.int/ihr/gcr-work-areas/en/.

[73] https://webgate.ec.europa.eu/chafea_pdb/health/projects/848096/summary.

State behaviour in cyberspace in international security context	
Funding projects aiming at increasing security and preparedness of critical information infrastructure and networks in third countries on the basis of a whole-of-government approach, while ensuring compliance with human rights and the rule of law	Regulation (EU) 230/2014 establishing an instrument contributing to stability and peace, OJ L 77, 15.3.2014, p. 1
Setting up of an EU External Cyber Capacity Building Network to mobilise collective MS expertise, support effective coordination for EU-funded external cyber capacity and increase training opportunities in partner countries	Communication from the Commission - A credible enlargement perspective for an enhanced EU engagement with the Western Balkans, COM(2018) 65 final EU-Western Balkans Sofia Declaration and Sofia Priority agency[74] , 17 May 2018 Multi-annual Action Plan on a Regional Economic Area in the Western Balkans- 12 July 2017 [75] Council Conclusions on EU External Cyber Capacity Building Guidelines – 26 June 2018[76] Eastern Partnership - 20 Deliverables for 2020 Focusing on key priorities and tangible results, SWD(2017) 300 final Joint Communication - Eastern Partnership policy beyond 2020 - Reinforcing Resilience - an Eastern Partnership that delivers for all, JOIN(2020) 7 final
Cyber dialogues with the US, Japan, Brazil, India, South Korea, China and Canada	
Cooperation with G7, Basel Committee on Banking Supervision, Financial Stability Board, Committee on Payments and Market Infrastructures on cybersecurity in the financial sector to explore solutions to better integrate cybersecurity into the financial services policy and regulatory landscape	G7 Fundamental principles of cybersecurity in the financial sector G7 Fundamental Elements for Threat-Led Penetration Testing G7 Fundamental Elements for Third Party Cyber Risk Management FSB Effective Practices for Cyber Incident Response and Recovery: Consultative document BCBS Cyber-resilience: range of practices

[74] https://www.consilium.europa.eu/media/34776/sofia-declaration_en.pdf.

[75] file:///C:/Users/buttimo/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/map_regional_economic_area_06_july_2017_clean_version.pdf.

[76] http://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.

20. EU-NATO cooperation

20.1 Staff-to-staff EU-NATO cooperation

Measure	Reference documents
Systematic staff-to-staff cooperation with NATO on StratCom, hybrid threats analysis (Parallel and Coordinated Assessments - PACA), bolstering, crisis prevention and response, cross briefings and expert discussions	Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation, 8 July 2016[77] Joint Declaration on EU-NATO cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation, July 2018 [78] Council Conclusions on the Implementation of the Joint Declaration, 6 December 2016[79] Council conclusions on the Implementation of the Joint Declaration, 5 December 2017[80] Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016, 14 June 2017[81] Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016, 29 November 2017[82] Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 31 May 2018[83]

[77] https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf.

[78] https://www.consilium.europa.eu/pl/press/press-releases/2018/07/10/eu-nato-joint-declaration/#.

[79] http://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf.

[80] https://www.consilium.europa.eu/media/31947/st14802en17.pdf.

[81] https://www.consilium.europa.eu/media/23997/170614-joint-progress-report-eu-nato-en.pdf.

[82] https://www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf.

[83] https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf.

	Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 17 June 2019[84] Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, 16 June 2020[85]
Coordination of training, cross-participation in exercises, joint workshops in cybersecurity with NATO and industry experts	Technical Arrangement on cyber defence between NATO's Computer Incident Response Capability (NCIRC) and CERT-EU
Parallel and Coordinated Exercises (PACE)	Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation, 8 July 2016[86] Joint Declaration on EU-NATO cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation, July 2018 [87]
20.2 Collaboration with the Centre of Excellence for Countering Hybrid Threats	
Measure	**Reference documents**
Establishment of the Centre of Excellence for Countering Hybrid Threats as well as continuous support and involvement in its work by the Commission and the European External Action Service	Memorandum of Understanding on the establishment of the Centre of Excellence for Countering Hybrid Threats (HCoE)[88]
Establishment of three Communities of Interests with sub-communities and various work strands and extensive networks in participating States	Memorandum of Understanding on the establishment of the HCoE
Developing expertise by the Centre in designing and organising high level exercises and scenario-based policy discussions	Memorandum of Understanding on the establishment of the HCoE
Workshops, seminars, conferences etc. on hybrid threats relevant topics with participation of representatives from EU institutions, including as speakers	Annual Work Programmes of the Centre of Excellence for Countering Hybrid Threats (2018, 2019, 2020)
EU-HYBNET: Pan-European network of practitioners coordinated by Laurea University Helsinki (incl. the Hybrid Centre of Excellence and the Commission's Joint Research Centre) to support security research on hybrid threats	Horizon 2020 Secure Societies Work Programme: General Matters
Joint scientific project on common understanding of hybrid threats	The Landscape of Hybrid Threats: A Conceptual Model, JRC117280

[84] https://www.consilium.europa.eu/media/39782/fourth-report-ue-nato-cooperation-en.pdf.

[85] https://www.consilium.europa.eu/media/44451/200616-progress-report-nr5-eu-nato-eng.pdf.

[86] https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf.

[87] https://www.consilium.europa.eu/pl/press/press-releases/2018/07/10/eu-nato-joint-declaration/#.

[88] https://www.hybridcoe.fi/wp-content/uploads/2017/08/Hybrid-CoE-final-Mou-110417-1.pdf.

21. Preventing, responding to crisis and recovering	
Measure	**Reference documents**
Facilitation and coordination of EU response mechanisms and early warning systems, in particular national civil protection, EU Integrated Political Crisis Response, ARGUS, European Emergency Response Coordination Centre, EEAS Crisis Response Mechanism and EEAS Situation Room on external security dimension, Strategic Analysis and Response Centre on internal security	EU operational protocol for countering hybrid threats "EU Playbook", SWD(2016) 227 final Commission Decision 2006/25/EC of 23 December 2005 amending its internal Rules of Procedure, OJ L 19, 24.1.2006, p. 20 and OJ L 118M, 8.5.2007, p. 76 Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism, OJ L 77I , 20.3.2019, p. 1 Commission Implementing Decision (EU) 2018/142 amending Implementing Decision 2014/762/EU laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism, OJ L 25, 30.1.2018, p. 40
Parallel and Coordinated Exercises (pilot PACE) in 2017 and 2018 - Exercises at working and political levels to test national and multinational decision-making ability, including a series of scenario-based policy discussions	PACE concept "Implementation of Parallel and Coordinated Exercises between NATO and the EU", 9 February 2017
Response to hybrid threats through solidarity and mutual assistance	Council Decision 2014/415/EU on the arrangements for the implementation by the Union of the solidarity clause, OJ L 192, 1.7.2014, p. 53
Gathering electronic evidence and improving cross-border access	Commission Proposal for Regulation on European production and preservation order for electronic evidence in criminal matters, COM (2018) 225 final Commission Proposal for Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226 final

22. EU institutional resilience

Measure	Reference documents
Enhancing the cooperation amongst Commission, EEAS, Council and European Parliament security departments through multilateral meetings on a variety of topics, including awareness raising, exchange of knowledge and experience and technical support	See Primary Documents on page 3
Regular intelligence-based analytical reporting by the EU Hybrid Fusion Cell on hostile intelligence activities (including cyber espionage) targeting the security of the EU Institutions and personnel	See Primary Documents on page 3
Enhancing resilience and improving security culture of the EU institutions against cyber and hybrid threats and better protection of the EU institutions' information and communication networks and its decision-making processes from malicious activities of all kinds. Since 2018, the Commission has taken the following measures: • Revamped the internal rules on protection of sensitive information; • Adopted principles on outsourcing of IT systems; • Adopted new implementing rules on handling classified information, on classified procurement; • Updated the IT system to handle RESTREINT UE/EU RESTRICTED information, in coordination with the EEAS; • Launched a project for a system to handle highly classified information in support of new policy priorities, to be deployed in autumn 2020; • Invested in staff awareness, with thousands of security briefings given to staff across the entire institution.	Communication Corporate Information Security Strategy, C(2019) 1834 Security Notice Security accreditation of communication and information systems handling EUCI, C(2019) 1890 Security Notice Information assessment and classification, C(2019) 1903 Security Notice Marking and handling of sensitive non-classified information, C(2019) 1904 Standard under Decision (EU, Euratom) 2017/46 Principles for outsourcing of communication and information systems, C(2020) 4190 Commission Decision (EU, Euratom) 2018/6575 on implementing rules for physical security measures aimed at protection European Union classified information Commission Decision (EU, Euratom) 2019/1961 of 17 October 2019 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information, OJ L 311, 2.12.2019, p. 1 Commission Decision (EU, Euratom) 2019/1962 of 17 October 2019 on implementing rules for handling RESTREINT UE/EU RESTRICTED information, OJ L 311, 2.12.2019, p. 21 Commission Decision (EU, Euratom) 2019/1963 of 17 October 2019 laying down implementing rules on industrial security with regard to classified

	procurement, OJ L 311, 2.12.2019, p. 37 Security Notice on the registration of CONFIDENTIAL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information for security purposes, C(2020) 4191